TLP:WHITE
REVISION: 1
PUBLICATION DATE: 2023-03-14
DOC. IDENTIFIER: 8DBD000142
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

CYBERSECURITY ADVISORY

Arbitrary code execution Vulnerability in Hitachi Energy's MicroSCADA Pro/X SYS600 Products

CVE-2011-1207

Notice

The information in this document is subject to change without notice and should not be construed as a commitment by Hitachi Energy. Hitachi Energy provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall Hitachi Energy or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if Hitachi Energy or its suppliers have been advised of the possibility of such damages. This document and parts hereof must not be reproduced or copied without written permission from Hitachi Energy and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose. All rights to registrations and trademarks reside with their respective owners.

Summary

Hitachi Energy is aware of the vulnerability CVE-2011-1207 in the Data Dynamics ActiveBar (ActBar) ActiveX Controls component, that affects the SYS600 versions listed below. Please refer to the Recommended Immediate Actions for information about the mitigation. A user who successfully exploits the vulnerability, could execute arbitrary code.

Vulnerability ID, Severity and Details

The vulnerability's severity assessment is performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1. The CVSS Environmental Score, which can affect the final vulnerability severity score, is not provided in this advisory as it reflects the potential impact of the vulnerability in the customer organizations' computing environment. Customers are recommended to analyze the impact of the vulnerability in their environment and calculate the CVSS Environmental Score.

Vulnerability ID	Detail Description
CVE-2011-1207 CVSS v3.1 Base Score: 6.7 Medium CVSS v3.1 Vector: AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H Link to NVD: click here CWE-264: Permissions, Privileges, and Access Controls	The ActiveBar ActiveX control distributed in ActBar.ocx 1.0.3.8 in SYS600 Product, does not properly restrict the SetLayoutData method, which allows attackers to execute arbitrary code via a crafted Data argument.

Recommended Immediate Actions

The Table below shows the affected version and the recommended immediate actions.

Affected Version	Recommended Actions
SYS600 9.4 FP2 Hotfix 5 and earlier	For SYS600 9.x: upgrade to at least SYS600 version 10.2 or apply general mitigation factors.
SYS600 10.1.1 and earlier	For SYS600 10.x update to at least SYS600 version 10.2 or apply general mitigation factors.

Hitachi Energy recommends that customers apply the update at the earliest convenience.

NOTE:
Even though the vulnerability is fixed in SYS600 10.2, some vulnerability scanners may continue to report the component as vulnerable, and this should be treated as a false positive.
From SYS600 10.5 onwards, the reason for the false identification is fixed.

General Mitigation Factors/Workarounds

Recommended security practices and firewall configurations can help protect a process control network from attacks that originate from outside the network. Such practices include that process control systems are physically protected from direct access by unauthorized personnel, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed, and others that have to be evaluated case by case. Process control systems should not be used for Internet surfing, instant messaging, or receiving e-mails. Portable computers and removable storage media should be carefully scanned for viruses before they are connected to a control system. Proper password policies and processes should be followed.

We recommend following the cybersecurity deployment guideline as follows: 1MRK511518 MicroSCADA X Cyber Security Deployment Guideline.

Frequently Asked Questions

What is SYS600?

SYS600 is a SCADA product, which is used for monitoring and controlling power systems.

What might an attacker use the vulnerability to do?

An attacker who successfully exploits this vulnerability can execute unauthorized code on the targeted device.

How could an attacker exploit the vulnerability?

To exploit the vulnerability of this component, an attacker needs to gain access to the system where SYS600 is integrated or trick the operator to download and open a malicious file.

Could the vulnerability be exploited remotely?

The vulnerability is not bound to a network stack. In order to exploit this vulnerability an attacker would need to have access to an affected system node.

When this security advisory was issued, had this vulnerability been publicly disclosed or could an attacker exploit the vulnerability?

Yes, this vulnerability has been publicly disclosed by the developer of the Actbar.ocx.

When this security advisory was issued, had Hitachi Energy received any report that this vulnerability was being exploited?

While an exploit to the CVE-2011-1207 is available [1,2], Hitachi Energy does not have information to indicate Hitachi's Energy's products have been exploited.

Reference

1. https://www.infosecmatter.com/nessus-plugin-library/?id=54841
2. https://www.exploit-db.com/exploits/4190

Support

This advisory will be updated as new relevant information becomes available. Please subscribe to Hitachi Energy’s Cybersecurity Alerts & Notifications to get notified:

https://www.hitachienergy.com/offering/solutions/cybersecurity/alerts-and-notifications/subscribe

For additional information and support please contact your product provider or Hitachi Energy service organization. For contact information, see https://www.hitachienergy.com/contact-us/ for Hitachi Energy contact-centers.

Publisher

Hitachi Energy PSIRT – cybersecurity@hitachienergy.com

Revision

Date of the Revision	Revision	Description
2023-03-14	1	Initial public release.

DocuSigned by:

Issued by: Hitachi Energy
Hitachi Energy
Product Security Incident Response Team